Helsinki 28.1.2004

E T U O I K E U S T O D I S T U S
P R I O R I T Y D O C U M E N T

Hakija Applicant	**Qitec Technology Group Oy** **Helsinki**
Patenttihakemus nro Patent application no	20030154
Tekemispäivä Filing date	31.01.2003
Kansainvälinen luokka International class	H04L
Keksinnön nimitys Title of invention	

REC'D · 20 APR 2004

WIPO   PCT

"Method and system for identifying the identy of a user"
(Menetelmä ja järjestelmä käyttäjän identiteetin tunnistamiseksi)

Täten todistetaan, että oheiset asiakirjat ovat tarkkoja jäljennöksiä Patentti- ja rekisterihallitukselle alkuaan annetuista selityksestä, patenttivaatimuksista, tiivistelmästä ja piirustuksista.

This is to certify that the annexed documents are true copies of the description, claims, abstract and drawings originally filed with the Finnish Patent Office.

Pirjo Kaila
Tutkimussihteeri

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

Maksu	50 €	
Fee	50 EUR	

Maksu perustuu kauppa- ja teollisuusministeriön antamaan asetukseen 1027/2001 Patentti- ja rekisterihallituksen maksullisista suoritteista muutoksineen.

The fee is based on the Decree with amendments of the Ministry of Trade and Industry No. 1027/2001 concerning the chargeable services of the National Board of Patents and Registration of Finland.

1 ~~2~~

METHOD AND SYSTEM FOR IDENTIFYING THE IDENTITY OF A USER

FIELD OF THE INVENTION

The present invention relates to communica-
5 tion systems. In particular, the present invention re-
lates to a novel and improved method and system for
identifying a user in a communication system.

BACKGROUND OF THE INVENTION

10 User identification is an essential procedure
for various tasks in the Internet environment. User
identification is needed in various environments, e.g.
in email login, on-line shopping, on-line banking etc.
There is always a fundamental problem to be solved
15 when using on-line identification methods, namely, how
to make sure that the person making the identification
is actually the person who he/she claims to be.

For identification purposes, several solu-
tions are used to solve the aforementioned problem. A
20 basic solution is to use a username and password. The
username/password combination is often adequate for
identification purposes but not always. Today, a num-
ber of services require user identification, and for
this reason, an individual may have tens of different
25 username/password pairs stored somewhere, e.g. in a
computer or a paper sheet in a drawer. Therefore,
sometimes these username/password pairs may end up to
people not authorized to use them, e.g. the computer
may be vulnerable for hacking or the drawer is too ob-
30 vious place to hide the username/password pairs.

There are also other identification solutions
used in on-line identification solutions. A user may
use one or more static piece of identification infor-
mation (e.g. username and/or password) but also a
35 varying piece of information (e.g. a varying PIN code)
is needed. This is the solution at least in several

?

on-line banking solutions. In these solutions, each session and/or transaction requires a predetermined varying identifier to be used.

5   The current discussion about identification solutions primarily concentrates on Internet-based solutions. This is of course important because data networks, such as the Internet, are always vulnerably to hostile attacks or hackers.

10   There are, however, also a number of on-line identification solutions used in telephone networks. There exists several phone services through which confidential information can be acquired or changed, e.g. telephone bank services, various health-related services, telephone operator services etc. In such serv-

15 ices, some kind of identification procedure is often used. A calling person can be identified e.g. based on the A-number (calling line identification), customer identification number, PIN code, username and/or password etc. These solutions are very similar to the ones

20 used in Internet-based solutions.

    All the aforementioned solutions have, however, some drawbacks. Some of these drawbacks will now be discussed shortly:

    <u>A-number (calling line identification)</u>: An A-

25 number identifies only the terminal or subscription from which the phone call is set up. It does not necessarily identify the calling person. It is always possible that someone fraudulently poses as being someone else.

30   <u>Personal Identification Number (PIN)</u>: A PIN code can be used alone or with e.g. the A-number in identification. It may be difficult, as previously mentioned, to remember PIN codes related to each service. Again it is possible that someone fraudulently

35 poses as being someone else.

    <u>Varying PIN code with a customer identification number</u>: This solution was discussed above

3

briefly. Systems based on using varying PIN code with a customer identification number are in itself reliable but expensive to set up, use and maintain. Solution of this kind is used at least by telephone banks
5   or other service providers using an up-to-date regular customer system.

Some of the services provided by the public sector or other (private or commercial) service providers have a need to implement a significant part of
10 the existing services via telephone voice connections. These services, however, require a reliable identification of an individual or customer before providing the service. Furthermore, some of the services provided by the public sector or other (private or com-
15 mercial) service providers via telephone voice connections require a digital signature from the individual or customer.

Therefore, there is particularly an obvious need for a reliable on-line telephone identification
20 solution with which a calling person can be identified prior to providing service via the telephone connection. The solution should be secure and above all, easy to use and adopt and widely available when needed.
25

SUMMARY OF THE INVENTION

The present invention describes a method and system for identifying the identity of a user of a first terminal in a communication system. The system
30 comprises at least a communication network, a first terminal associated with the communication network, a service provider associated with the communication network and a certificate service provider. Furthermore, the first terminal preferably refers to a mobile
35 phone.

In the method, a first logical channel is set up from the first terminal to the service provider.

4

The service provider refers e.g. to a bank, police, post office, operator, credit card company, insurance company, telephone bank, social insurance institution etc. The identity of the user of the first terminal is
5   then identified via a second logical channel other than the established first logical channel between the service provider and the first terminal prior to providing any services to the user of the first terminal via the established first logical channel. In other
10 words, the present invention uses a second logical channel to identify the identity of the user of a first terminal. The logical channels may be circuit switched or packet switched. Furthermore, the user may be identified by a separate party via the second logi-
15 cal channel, the party being other than the user of the first terminal.

In one embodiment, the communication network is a mobile telephone network. In one embodiment, the first and/or second logical channel refers to the
20 standardized GSM network data transmission feature that can be used simultaneously during a circuit switched speech connection. In other embodiments, the logical channels may refer e.g. to transmission channels of a GPRS, UMTS, WCDMA, CDMA, EDGE, Bluetooth,
25 WLAN network or to any other existing or future data transmission network.

In one embodiment of the present invention, the service provider sends a user identification request to the first terminal via a second logical chan-
30 nel (e.g. via a packet switched connection) while a first logical channel exists between the first terminal and the service provider. The request is prefera-bly sent to the first terminal directly and more pref-erably, using a security gateway forming an interface
35 towards the first terminal. The request is preferably encrypted. The first terminal receives the request and decrypts it if encryption was used. In order to give

5

an adequate indication of the identity of the user of
the first terminal, the request is signed digitally by
the first terminal.

In order to create a digital signature, the
5   first and/or second terminals need to comprise an en-
cryption key, and furthermore in order to create the
digital signature, the user of a terminal must have a
correct pass phrase or PIN code to activate the signa-
ture creation. The signed identification request is
10   then sent either directly to the service provider or
more preferably, to the security gateway. The signed
request may also be encrypted by the first and/or sec-
ond terminal.

The digital signature is then verified based
15   on a certificate corresponding to the authentication
key used in creating the digital signature, the cer-
tificate being acquired from a certificate service
provider or other service provider. The verification
is preterably made by the service provider, and more
20   preferably, by the security gateway. If the user is
properly authenticated and the result of the verifica-
tion is positive, the user of the first terminal may
now be provided with services provided by the service
provider via the existing first logical channel.

25   For some reason, the set up first logical
channel may fail while the identification and valida-
tion process is still unfinished. Therefore, a proce-
dure for re-establishing a validated connection has to
be provided. If the first logical channel fails during
30   the verification procedure, the service provider cre-
ates a challenge, e.g. a password, and encrypts it us-
ing the public encryption key of the user of the first
terminal. The encrypted challenge is then sent to the
first terminal either directly or more preferably, us-
35   ing the security gateway. The first terminal decrypts
the encrypted challenge, sets up a new logical channel
to the service provider and provides the service pro-

6

vider with the decrypted challenge. If the challenge
is acceptable, the user of the first terminal is pro-
vided via rhe re-established logical channel with a
service by the service provider.

5   The present invention enables a reliable
identification of an individual or a customer over a
logical channel, e.g. a telephone line. The present
invention provides a solution wherein multiple serv-
ices can use the same security solution for authenti-

10 cation, authorization, administration and access con-
trol. Furthermore, the solution is cost-efficient, se-
cure and easy to implement into the existing systems.

BRIEF DESCRIPTION OF THE DRAWINGS

15   The accompanying drawings, which are included
to provide a further understanding of the invention
and constitute a part of this specification, illus-
trate embodiments of the invention and together with
the description help to explain the principles of the

20 invention. In the drawings:
         Fig 1 is a flow diagram illustrating a user
identification procedure in accordance with the pres-
ent invention,
         Fig 2 is a flow diagram illustrating a user

25 identification procedure in accordance with the pres-
ent invention,
         Fig 3 is a flow diagram illustrating a re-
establishing procedure in accordance with the present
invention,

30   Fig 4 is a flow diagram illustrating a user
identification procedure in accordance with the pres
ent invention,
         Fig 5 is a flow diagram illustrating a re-
establishing procedure in accordance with the present

35 invention,

7

Fig 6 is a flow diagram illustrating a user identification procedure in accordance with the present invention,

Fig 7 is a flow diagram illustrating a user
5   identification procedure in accordance with the present invention,

Fig 8 is a flow diagram illustrating a user identification procedure in accordance with the present invention, and
10   Fig 9 is a block diagram of an embodiment of the system in accordance with the present invention.

DETAILED DESCRIPTION OF THE INVENTION

Reference will now be made in detail to the
15   embodiments of the present invention, examples of which are illustrated in the accompanying drawings.

In the following examples, a user is considered to be a user making a phone call. It is evident that the call connection may be any other appropriate
20   logical channel or connection (e.g. a packet switched channel or connection) between a user terminal and a service provider.

Figure 1 describes an embodiment of a user identification procedure. A call connection is set up
25   (10) from a caller terminal DTE to a service number of a service provider SP via a communication network NET. The service provider SP refers e.q. to a bank, police, post office, operator, credit card company, insurance company, telephone bank or social insurance institu-
30   tion. It may, however, be any other company or insti- tution that provides services requiring undisputed identification of the caller. In Figure 1, the service provider SP comprises at least a service provider server/exchange SPS, customer database DB and customer
35   servant SERV. The communication network NET is pref- erably a mobile telephone network. The caller terminal

8

DTE is preferably a mobile phone comprising a sub-
scriber identity module SIM. Instead of a subscriber
identity module SIM, a Wireless Identity Module (WIM),
an UMTS Subscriber Identity Module (USIM), a security
5   module or any other tamper-proof device can be used.
The subscriber identity module SIM or any other tam-
per-proof device enables encryption and decryption of
information and also forming of a digital signature.
In a preferred embodiment, the subscriber identity
10   module SIM or any pother tamper-proof device also com-
prises a storage for encryption and/or decryption
keys. Furthermore, in a preferred embodiment, Public
Key Infrastructure (PKI) is used in encryption and de-
cryption.

15   The service provider server SPS sends a
caller identification request (11) to a security gate-
way GW. In Figure 1, the security gateway GW is owned
by the operator of the communication network NET and
it provides various security-related functions, such
20   as encrypting and decrypting. The request (11) is
transmitted to the security gateway GW through a se-
cured connection (e.g. Secured Sockets Layer (SSL))
e.g. in the form of HyperText Transfer Protocol
(HTTP), Wireless Markup Language (WML) or Extensible
25   Markup Language (XML).

         It is very important to note that, in this
embodiment, the call connection is maintained during
the identification phase.

         The security gateway GW identifies the serv-
30   ice provider SP based on a service provider certifi-
cate, decrypts the secured connection and receives the
caller identification request in clear text e.g. in
the form of XML, WML or short message. The caller
identification request is then converted into a form
35   understood by the subscriber identity module SIM of
the mobile terminal DTE and encrypted with symmetric
encryption method of the Global System for Mobile com-

9

municacions (GSM). The encrypted message is then sent (12) to the mobile phone DTE.

The mobile phone DTE and/or the subscriber identity module SIM decrypt(s) the message and the de-
5   crypted message is displayed to the caller on the display of the mobile phone DTE. The subscriber identity module SIM may comprise a browser that converts the message into SIM Toolkit commands prior to displaying the message on the display. The displayed message is
10 then digitally signed with an authentication key of the caller, and the signed message is sent (13) to the security gateway GW. The signed message is preferably converted into the form Public-Key Cryptography Standards #1 (PKCS#1) and encrypted prior to sending.
15 PKCS#1 is further described e.g. in http://www.rsasecurity.com/rsalabs/pkcs/.

The security gateway GW decrypts the message and fetches (14) a certificate related to the subscriber from a certificate directory DIR of a certifi-
20 cate authority CA. The certificate authority CA maintains one or more certificate directories and a certificate revocation list CLR comprising information about revoked certificates. A certificate comprises identification information of the certificate owner
25 and above all, the public key of the owner. With the public key it is possible to verify a digital signature. Verification process refers to a process performed by a verifier either soon after the creation of an electronic signature or later to determine if an
30 electronic signature is valid against a signature policy implicitly or explicitly referenced. Verification is linked very strongly to the term 'validation data'. Validation data refers to the additional data needed to validate the electronic signature; this includes
35 e.g. certificates, revocation status information (e.g. CRLs) and trusted time-stamps. Furthermore, the security gateway GW creates a PKCS#7 message and sends

10

(15) the message to the service provider SP preferably using a secured connection. PKCS#7 is further described   e.g.   in http://www.rsasecurity.com/rsalabs/pkcs/.

5   The service provider SP authenticates the caller and verifies (16) the digital signature and checks from the certificate revocation list CLR that the certificate is valid. If the verification procedure was successful, the caller may now be provided

10   the requested service. Furthermore, the service provider may create a data record containing the caller information (17) from the database DB, validation information and a call log information. Call log information simply indicates that the call had existed

15   during the identification procedure. The customer servant SERV preferably uses a computer, and therefore, is automatically provided (18) with the aforementioned data record prior to talking to the caller.

        Figure 2 describes another embodiment of a

20   user identification procedure. A call is set up (20) from a caller terminal DTE to a service number of a service provider SP via a communication network NET. The service provider SP refers e.g. to any private, commercial or state-owned institution. e.g. to a bank,

25   police, post office, operator, credit card company, insurance company, telephone bank or social insurance institution. It may, however, be any other company or institution that provides services requiring undisputed identification of the caller. In Figure 2, the

30   service provider SP comprises at least a service provider server/exchange SPS, customer database DB and customer servant SERV. The communication network NET is preferably a mobile telephone network. The caller terminal DTE is preferably a mobile phone comprising a

35   subscriber identity module SIM. Instead of a subscriber identity module SIM, a Wireless Identity Module (WIM), an UMTS Subscriber Identity Module (USIM),

11

a security module or any other tamper-proof device can
be used. The subscriber identity module SIM or any
other tamper-proof device enables encryption and de-
cryption of information and also forming of a digital
5   signature. In a preferred embodiment, the subscriber
identity module SIM also comprises a storage for en-
cryption and/or decryption keys. Furthermore, in a
preferred embodiment, Public Key Infrastructure (PKI)
is used in encryption and decryption.

10   The service provider SPS sends a caller iden-
tification request (21) to a security gateway GW. In
Figure 2, the security gateway GW is owned by the op-
erator of the communication network NET and it pro-
vides various security-related functions, such as en-
15   crypting and decrypting. The request (21) is transmit-
ted to the security gateway GW through a secured con-
nection (e.g. Secured Sockets Layer (SSL)) e.g. in the
form of HyperText Transfer Protocol (HTTP), Wireless
Markup Language (WML) or Extensible Markup Language
20   (XML).

        It is very important to note that the call
connection is maintained during the identification
phase.

        The security gateway GW identifies the serv-
25   ice provider SP based on a service provider certifi-
cate, decrypts the secured connection and receives the
caller identification request in clear text e.g. in
the form of XML, WML or short message. The caller
identification request is then converted into a form
30   understood by the subscriber identity module SIM of
the mobile terminal DTE and encrypted with symmetric
encryption method of the Global System for Mobile com-
munications (GSM). The encrypted message is then sent
(22) to the mobile phone DTE.

35   The mobile phone DTE and/or the subscriber
identity module SIM decrypt(s) the message and the de-
crypted message is displayed to the caller on the dis-

12

play of the mobile phone DTE. The subscriber identity
module SIM may comprise a browser that converts the
message into SIM Toolkit commands prior to displaying
the message on the display. The displayed message is
5   then digitally signed with an authentication key of
the caller and the signed message is sent (23) to the
security gateway GW. The signed message is preferably
converted into the form Public-Key Cryptography Stan-
dards #1 (PKCS#1) and encrypted prior to sending.
10 PKCS#1   is   further   described   e.g.   in
http://www.rsasecurity.com/rsalabs/pkcs/.
        The security gateway GW decrypts the message
and fetches (24) a certificate related to the sub
scriber from a certificate directory DIR of a certifi-
15 cate authority CA. The certificate authority CA main-
tains one or more certificate directories and a cer-
tificate revocation list CLR comprising information
about revoked certificates. The certificate authority
CA may also comprise information about which users are
20 authorized for one or more services and which are not.
A certificate comprises identification information of
the certificate owner and above all, the public key of
the owner. With the public key it is possible to ver-
ify a digital signature. The security gateway GW veri-
25 fies the digital signature and checks from the cer-
tificate revocation list CLR that the certificate is
valid. If the verification procedure was successful,
the security gateway GW sends (25) verification posi-
tive message to the service provider SP preferably us-
30 ing a secured connection. The service provider server
then creates a data record containing the caller in-
formation (26) from a database DB, validation informa
tion and a call log information. Call log information
simply indicates that the call had existed during the
35 identification procedure. The customer servant SERV
preferably uses a computer, and therefore, is auto-

13

matically provided (27) with the aforementioned data
record prior to talking to the caller.

Figure 3 describes an embodiment in which the
originally establish call connection fails and the
5   call connection is re-established.

When the service provider server SPS detects
that the call connection does not exist any more, it
creates a challenge. A challenge is any piece of in-
formation containing e.g. alphanumeric characters. The
10 challenge is then encrypted using the public key of
the caller. The public key is acquired from a previous
PKCS#7 message, or if such message has not been re-
ceived, from a public certificate directory. After
this, the service provider server SPS sends (30) the
15 encrypted challenge via the security gateway GW to the
caller terminal DTE that is preferably a mobile phone
(31).

The example described in Figure 3 assumes
that the caller identity was already identified and
20 validated before and that the original call connection
failed. Therefore, after sending the encrypted chal-
lenge to the caller, the service provider server SPS
sets the validated identification data into a hold
state.

25   The mobile phone DTE and/or the subscriber
identity module SIM or alike incorporated therein de-
crypt(s) the encrypted challenge and sets (32) up a
new call connection to the service provider SP. The
exchange SPS redirects (33) the call to a customer
30 servant SERV and provides the customer servant SERV
with the already validated identification information
and the challenge sent to the caller. If the caller
then gives the right challenge to the customer ser-
vant, the caller may be provided with the service in
35 question.

Figure 4 describes another embodiment of a
user verification procedure. A call is set up (40)

14

from a caller terminal DTE to a service number of a
service provider SP via a communication network NET.
The service provider SP refers e.g. to any private,
commercial or state-owned institution, e.g. to a bank,
5   police, post office, operator, credit card company,
insurance company, telephone bank or social insurance
institution. It may, however, be any other company or
institution that provides services requiring undis-
puted identification of the caller. In Figure 4, the
10   service provider SP comprises at least a service pro-
vider server/exchange SPS, customer database DB and
customer servant SERV. The communication network NET
is preferably a mobile telephone network. The caller
terminal DTE is preferably a mobile phone comprising a
15   subscriber identity module SIM. Instead of a sub-
scriber identity module SIM, a Wireless Identity Mod
ule (WIM), an UMTS Subscriber Identity Module (USIM),
a security module or any other tamper-proof device can
be used. The subscriber identity module SIM or any
20   other tamper-proof device enables encryption and de-
cryption of information and also forming of a digital
signature.

The service provider exchange SPS connects
(41) the call to a free customer servant SERV. After
25   that the customer servant SERV transmits (42) a caller
identification request to the security gateway GW. In
Figure 4, the security gateway GW is owned by the op-
erator of the communication network NET and it pro
vides various security-related functions, such as en-
30   crypting and decrypting. The request is transmitted to
the security gateway GW through a secured connection
(e.g. Secured Sockets Layer (SSL)) e.g. in the form of
HyperText Transfer Protocol (HTTP), Wireless Markup
Language (WML) or Extensible Markup Language (XML).
35   It is very important to note that the call
connection is maintained during the identification
phase.

15

The security gateway GW identifies the service provider SP based on a service provider certificate, decrypts the secured connection and receives the caller identification request in clear text e.g. in the form of XML, WML or short message. The caller identification request is then converted into a form understood by the subscriber identity module SIM of the mobile terminal DTE and encrypted with symmetric encryption method of the Global System for Mobile communications (GSM). The encrypted message is then sent (43) to the mobile phone DTE.

The mobile phone DTE and/or the subscriber identity module SIM decrypt(s) the message and the decrypted message is displayed to the caller on the display of the mobile phone DTE. The subscriber identity module SIM may comprise a browser that converts the message into SIM Toolkit commands prior to displaying the message on the display. The displayed message is then digitally signed with an authentication key of the caller, and the signed message is sent (44) to the security gateway GW. The signed message is preferably converted into the form Public-Key Cryptography Standards #1 (PKCS#1) and encrypted prior to sending. PKCS#1 is further described e.g. in http://www.rsasecurity.com/rsalabs/pkcs/.

The security gateway GW decrypts the message and fetches (45) a certificate related to the subscriber from a certificate directory DIR of a certificate authority CA. The certificate authority CA maintains one or more certificate directories and a certificate revocation list CLR related to revoked or unusable certificates. The certificate authority CA may also comprise information about which users are authorized for one or more services and which are not. The term authorization itself refers to the process of giving someone permission to do or have something. A certificate comprises identification information of

16

the certificate owner and above all, the public key of the owner. With the public key it is possible to ver ify a digital signature. Furthermore, the security gateway GW creates a PKCS#7 message and sends (46) the
5 message directly to the customer servant SERV preferably using a secured connection. PKCS#7 is further described   e.g.   in http://www.rsasecurity.com/rsalabs/pkcs/.

The customer servant SERV verifies (47) the
10 digital signature and checks from the certificate revocation list CLR that the certificate is valid. If the verification procedure was successful, the caller may now be provided with the requested service after fetching (48) the caller-related information from a
15 customer database DB.

As described with Figure 4, the verification procedure and validation of the caller may in another embodiment be in its entirety implemented in the security gateway GW.
20   Figure 5 describes an embodiment in which the originally establish call connection fails and the call connection is re-established.

When the customer servant SERV realizes that the call connection does not exist any more, it cre-
25 ates a challenge. A challenge is any piece of information containing e.g. alphanumeric characters. The challenge is then encrypted using the public key of the caller. The public key is acquired from a previous PKCS#7 message or if such message has not been re-
30 ceived from a public certificate directory. After this the encrypted challenge is sent (50) via the security gateway GW to (51) the caller terminal DTE which is preferably a mobile phone.

The example described in Figure 5 assumes
35 that the caller identity was already identified and validated before and that the original call connection failed after that. Therefore, after sending the en-

17

crypted challenge to the caller, the customer servant
SERV sets the validated identification data into a
hold state.

The mobile phone DTE and/or the subscriber
5   identity module SIM or alike incorporated therein de-
crypts the encrypted challenge and sets (52) up a new
call connection directly to the customer servant SERV.
If the caller then gives the right challenge to the
customer servant, caller-related information is
10   fetched (53) from a database and the caller may be
provided with the service in question.

Figure 6 describes an embodiment of a user
identification procedure. In Figure 6, the security
gateway GW is property of the service provider SP.
15   A call is set up (60) from a caller terminal
DTE to a service number of a service provider SP via a
communication network NET. The service provider SP re-
fers e.g. to a bank, police, post office, operator,
credit card company, insurance company, telephone bank
20   or social insurance institution. It may, however, be
any other company or institution that provides serv
ices requiring undisputed identification of the
caller. In Figure 6, the service provider SP comprises
at least a service provider server/exchange SPS, the
25   security gateway GW, customer database DB and customer
servant SERV. The communication network NET is pref-
erably a mobile telephone network. The caller terminal
DTE is preferably a mobile phone comprising a sub-
scriber identity module SIM, a Wireless Identity Mod-
30   ule (WIM), an UMTS Subscriber Identity Module (USIM),
a security module or any other tamper-proof device.
The subscriber identity module SIM or any other tam-
per-proof device enables encryption and decryption of
information and also forming of a digital signature.
35   The caller must, however, be properly identi-
fied before providing any services to the caller.
Therefore, the security gateway GW in connection with

18

the service provider server SPS sends a caller identification request to the security gateway GW. The security gateway GW provides various security-related functions, such as encrypting and decrypting. The re-
5   quest (61) is transmitted to mobile phone DTE through a secured connection (e.g. Secured Sockets Layer (SSL)) e.g. in the form of HyperText Transfer Protocol (HTTP), Wireless Markup Language (WML) or Extensible Markup Language (XML) or a message of any other form
10   that may be secured or encrypted. The encryption method used can by symmetric or asymmetric.

It is very important to note that the call connection is maintained during the identification phase.

15   The mobile phone DTE and/or the subscriber identity module SIM decrypt(s) the message and the decrypted message is displayed to the caller on the display of the mobile phone DTE. The subscriber identity module SIM may comprise a browser that converts the
20   message into SIM Toolkit commands prior to displaying the message on the display. The displayed message is then digitally signed with an authentication key of the caller and the signed message is sent (62) back to the security gateway GW. The signed message is pref-
25   erably converted into the form Public-Key Cryptography Standards #1 (PKCS#1) and encrypted prior to sending.

In another embodiment of Figure 6, the mobile phone itself creates a PKCS#7 message and sends (62) it to the security gateway GW. The message can addi-
30   tionally be encrypted before sending.

The security gateway GW decrypts the message and fetches (63) a certificate related to the subscriber from a certificate directory DIR of a certificate authority CA. The certificate authority CA main-
35   tains one or more certificate directories and a certificate revocation list CLR related to revoked or unusable certificates. The certificate authority CA may

19

also comprise information about which users are authorized for one or more services and which are not. The term authorization itself refers to the process of giving someone permission to do or have something. A
5 certificate comprises identification information of the certificate owner and above all, the public key of the owner. With the public key it is possible to verify a digital signature.

The security gateway GW verifies the digital
10 signature and checks from the certificate revocation list CLR that the certificate is valid. If the verification procedure was successful, the caller may now be provided the requested service. Furthermore, the service provider server SPS may create a data record con-
15 taining the caller information (64) from a database DB, validation information and a call log information. Call log information simply indicates the call has been established during the identification procedure. The customer servant SERV preferably uses a computer,
20 and therefore, is automatically provided (65) with the aforementioned data record prior to talking to the caller.

Figure 7 describes an embodiment of a user identification procedure. In Figure 7, the security
25 gateway GW is property of the service provider SP. Furthermore, in Figure 7 the caller is identified by a second party.

A call is set up (70) from a caller terminal DTE to a service number of a service provider SP via a
30 communication network NET. The service provider SP refers e.g. to a bank, police, post office, operator, credit card company, insurance company, telephone bank or social insurance institution. It may, however, be any other company or institution that provides serv-
35 ices requiring undisputed identification of the caller. In Figure 7, the service provider SP comprises at least a service provider server/exchange SPS, the

20

security gateway GW, customer database DB and customer
servant SERV. The communication network NET is pref-
erably a mobile telephone network. The caller terminal
DTE is preferably an ordinary phone or a mobile phone
5   comprising a subscriber identity module, a wireless
identity module, an UMTS subscriber identity module, a
security module or any other tamper-proof device.

The caller must, however, be properly identi-
fied before providing any services to the caller.
10   Therefore, the security gateway GW in connection with
the service provider server SPS sends a caller identi-
fication request to a security gateway GW. The secu-
rity gateway GW provides various security-related
functions, such as encrypting and decrypting. The re-
15   quest (71) is then transmitted to a second terminal
DTE2 through a secured connection (e.g. Secured Sock-
ets Layer (SSL)) e.g. in the form of HyperText Trans-
fer Protocol (HTTP), Wireless Markup Language (WML) or
Extensible Markup Language (XML) or a message of any
20   other form that may be secured or encrypted. The en-
cryption method used can by symmetric or asymmetric.
The second terminal DTE2 is preferably a mobile phone
comprising a subscriber identity module, a wireless
identity module, an UMTS subscriber identity module, a
25   security module or any other tamper-proof device. How
ever, the second terminal DTE2 may refer to any other
terminal, e.g. a computer or Personal Data Assistant
(PDA), that can be used in identifying the identity of
the caller. The second terminal must therefore com-
30   prise means for encrypting and/or signing messages.

The second mobile phone DTE2 and/or the sub-
scriber identity module SIM decrypt(s) the message,
and the decrypted message is displayed to the user on
the display of the second mobile phone DTE2. The sub-
35   scriber identity module SIM may comprise a browser
that converts the message into SIM Toolkit commands
prior to displaying the message on the display. The

21

displayed message is then digitally signed with an
authentication key of the user and the signed message
is sent (72) back to the security gateway GW. The
signed message is preferably converted into the form
5   Public-Key Cryptography Standards #1 (PKCS#1) and en-
crypted prior to sending.

In another embodiment of Figure 7, the mobile
phone itself creates a PKCS#7 message and sends (72)
it to the security gateway GW. The message can addi-
10 tionally be encrypted before sending.

The security gateway GW decrypts the message
and fetches (73) a certificate related to the user of
the second mobile phone DTE2 from a certificate direc-
tory DIR of a certificate authority CA. The certifi-
15 cate authority CA maintains one or more certificate
directories and a certificate revocation list CLR re-
lated to revoked or unusable certificates. The cer-
tificate authority CA may also comprise information
about which users are authorized for one or more serv-
20 ices and which are not. The term authorization itself
refers to the process of giving someone permission to
do or have something. A certificate comprises identi-
fication information of the certificate owner and
above all, the public key of the owner. With the pub-
25 lic key it is possible to verify a digital signature.

The security gateway GW verifies the digital
signature and checks from the certificate revocation
list CLR that the certificate is valid. If the verifi-
cation procedure was successful, the caller may now be
30 provided the requested service. Furthermore, the serv-
ice provider server SPS may create a data record con-
taining the caller information (74) from a database
DB, validation information and a call log information.
Call log information simply indicates the call has
35 been established during the identification procedure.
The customer servant SERV preferably uses a computer,
and therefore, is automatically provided (75) with the

22

aforementioned data record prior to talking to the
caller.

As described in Figure 7, the caller is veri-
fied by another person via the logical channel. In a
5   preferred embodiment, the first logical channel exists
while the identifying the identity of the user of the
first terminal via the second logical channel. There-
fore is possible that the actual caller can be practi-
cally anybody but the identification must be acquired
10   from a predetermined party.

In another embodiment of Figure 7, the first
logical channel between the first terminal and the
service provider does not exist while identifying pro-
cedure of the identity of the user of the first termi-
15   nal DTE is made via the second logical channel. In one
embodiment, the user of the first terminal DTE sends a
service request (70) to the service provider SP. The
service request is e.g. a bank transaction request.
The request will not be accepted until an authoriza-
20   tion is received from a second terminal DTE2. For ac
quiring the authorization, the service provider SP
sends a user identification request of the user of the
first terminal DTE to the second terminal DTE2 (71).
The user identification is the digitally signed by the
25   second terminal DTE and/or the subscriber identity
module and the signed message is sent back to the
service provider (72). If the verification process
(73, 74) of the digital signature is positive, the
service request placed by the user of the first termi-
30   nal DTE can be accepted (75).

In this embodiment, the first terminal DTE
refers e.g. to an ordinary telephone, a mobile phone,
a computer or a Personal Data Assistant (PDA). There-
fore, the aforementioned service request may be made
35   via a phone call, email, short message service or any
other messaging system. The second terminal DTE2 is
preferably a mobile phone comprising a subscriber

23

identity module, a wireless identity module, an UMTS
subscriber identity module, a security module or any
other tamper-proof device. However, the second termi-
nal DTE2 may refer to any other terminal, e.g. a com-
5   puter or Personal Data Assistant (PDA), that can be
used in identifying the identity of the caller. The
second terminal DTE2 must therefore comprise means for
encrypting and/or signing messages.

Figure 8 describes an embodiment of a user
10   identification procedure. In Figure 8, the security
gateway GW is property of the service provider SP.
Furthermore, in Figure 8 the caller is identified by a
second party.

A call is set up (80) or a message is sent
15   from a user terminal DTE to a service provider SP via
a communication network NET. A service request is made
via the call or message. In this embodiment, the first
logical channel between the user terminal DTE and the
service provider SP may not exist while identifying
20   procedure of the identity of the user of the first
terminal DTE is made via the second logical channel.
The service provider SP refers e.g. to a bank, police,
post office, operator, credit card company, insurance
company, telephone bank or social insurance institu-
25   tion. It may, however, be any other company or insti-
tution that provides services requiring undisputed
identification of the caller. In Figure 8, the service
provider SP comprises at least a service provider
server/exchange SPS, the security gateway GW, customer
30   database DB and customer servant SERV. The communica-
tion network NET is preferably a mobile telephone net-
work. The user terminal DTE is e.g. an ordinary tele-
phone, or more preferably a mobile phone comprising a
subscriber identity module, a wireless identity mod-
35   ule, an UMTS subscriber identity module, a security
module or any other tamper-proof device.

24

The user must, however, be properly identi-
fied before providing any services to the user. There-
fore, the security gateway GW in connection with the
service provider server SPS sends a user identifica-
5   tion request to a security gateway GW. The request
comprises also a challenge. A challenge is any piece
of information containing e.g. alphanumeric charac-
ters. The security gateway GW provides various secu-
rity-related functions, such as encrypting and de-
10 crypting. The request (A1) is then transmitted to a
second terminal DTE2 through a secured connection
(e.g. Secured Sockets Layer (SSL)) e.g. in the form of
HyperText Transfer Protocol (HTTP), Wireless Markup
Language (WML) or Extensible Markup Language (XML) or
15 a message of any other form that may be secured or en-
crypted. The second terminal DTE2 is preferably a mo-
bile phone comprising a subscriber identity module, a
wireless identity module, an UMTS subscriber identity
module, a security module or any other tamper-proof
20 device. The encryption method used can by symmetric or
asymmetric.

The second mobile phone DTE2 and/or the sub-
scriber identity module SIM decrypt(s) the message
comprising also the challenge, and the decrypted mes-
25 sage is displayed to the user on the display of the
second mobile phone DTE2. The subscriber identity mod-
ule SIM may comprise a browser that converts the mes-
sage into SIM Toolkit commands prior to displaying the
message on the display. The displayed message compris-
30 ing the challenge is then digitally signed with an
authentication key of the user and the signed message
is sent (B2) back to the security gateway GW. The
signed message is preferably converted into the form
Public-Key Cryptography Standards #1 (PKCS#1) and en-
35 crypted prior to sending.

In another embodiment of Figure 8, the second
mobile phone itself DTE2 creates a PKCS#7 message and

25

sends (82) it to the security gateway GW. The message
can additionally be encrypted before sending.

　　　　After signing and sending the signed message
to the service provider SP, the user of the second mo-
5　bile phone DTE2 provides the challenge to the user of
the first terminal DTE (83). The user of the first
terminal DTE is provided with the challenge e.g. via a
phone call, short message service, email etc. If the
original connection (80) does not exist any more, the
10　user of the first terminal DTE sets up another call
(84) or sends another message to the service provider
SP via the communication network NET. The user must
provide the service provider with the challenge ac-
quired from the user of the second mobile phone DTE2.

15　　　　　The security gateway GW decrypts the message
and fetches (85) a certificate related to the user of
the second mobile phone DTE2 from a certificate direc-
tory DIR of a certificate authority CA. The certifi-
cate authority CA maintains one or more certificate
20　directories and a certificate revocation list CLR re-
lated to revoked or unusable certificates. The cer-
tificate authority CA may also comprise information
about which users are authorized for one or more serv-
ices and which are not. The term authorization itself
25　refers to the process of giving someone permission to
do or have something. A certificate comprises identi-
fication information of the certificate owner and
above all, the public key of the owner. With the pub-
lic key it is possible to verify a digital signature.

30　　　　　The security gateway GW verifies the digital
signature and checks from the certificate revocation
list CLR that the certificate is valid. If the verifi-
cation procedure was successful, the caller may now be
provided the requested service. Furthermore, the serv-
35　ice provider server SPS may create a data record con
taining the user information (86) from a database DB
and validation information. The customer servant SERV

26

preferably uses a computer, and therefore, is auto-
matically provided (87) with the aforementioned data
record prior to talking to the caller.

In this embodiment, the first terminal refers
5   e.g. to an ordinary telephone, a mobile phone, a com-
puter or a Personal Data Assistant (PDA). Therefore,
the aforementioned service request may be made via a
phone call, email, short message service or any other
messaging system. The second terminal DTE2 is prefera-
10 bly a mobile phone comprising a subscriber identity
module, a wireless identity module, an UMTS subscriber
identity module, a security module or any other tam-
per-proof device. However, the second terminal DTE2
may refer to any other terminal, e.g. a computer or
15 Personal Data Assistant (PDA), that can be used in
identifying the identity of the user of the first ter-
minal DTE. The second terminal DTE2 must therefore
comprise means for encrypting and/or signing messages.

Figure 9 describes an example of a preferred
20 system in accordance with the present invention. The
system comprises a communication network NET, a caller
terminal DTE associated with the communication network
NET and a service provider SP associated with the com-
munication network NET. The caller terminal DTE is
25 preferably a mobile phone and the communication net-
work NET a GSM network, a GSM network with a GPRS fea-
ture or an UMTS network.

The system further comprises a service pro-
vider server/exchange SPS and a customer servant SERV.
30 The customer servant SERV provides a caller with a
service. Furthermore, the system comprises a security
gateway GW that is used to provide various security
functions in the system, e.g. encrypting and decrypt-
ing. The system comprises also a certificate authority
35 CA that has access both to a certificate directory and
certificate revocation list CLR.

27

Sending means SM for sending a caller identification request are arranged in the service provider server/exchange SPS. The service provider server/exchange SPS furthermore comprises first en-
5 crypting means EN1 for encrypting information, first decrypting means DE1 for decrypting information and identifying means ID for identifying the caller after a call has been set up prior to providing any services to the caller based on the information provided by the
10 certificate authority CA. The aforementioned sending means SM are arranged also to send a challenge to the caller terminal DTE in the event that the telephone connection set up between the caller terminal DTE and service provider SP fails. In one embodiment, the
15 aforementioned sending means SM are arranged also to send a challenge to the second terminal DTE2.

The security gateway GW comprises sending means SM for sending a caller identification request, identifying means ID for identifying the caller after
20 a call has been set up prior to providing any services to the caller based on the information provided by the certificate authority CA. second encrypting means EN2 for encrypting information and second decrypting means DE2 for decrypting information.
25 The caller terminal DTE comprises a subscriber identity module SIM, third encrypting means EN3 for encrypting information and third decrypting means DE3 for decrypting information. Instead of a subscriber identity module SIM, a Wireless Identity
30 Module (WIM), an UMTS Subscriber Identity Module (USIM), a security module or any other tamper-proof device can be used. The subscriber identity module SIM or any other tamper-proof device enables encryption and decryption of information and also forming of a
35 digital signature.

The aforementioned means are implemented e.g. by software and/or hardware in a way known to skilled

28

in art and therefore they are not described in more detail.

Figures 1 - 9 disclose different configurations of the system in accordance with the present invention. In Figures 1 - 9, the certificate authority acts as a certificate service provider. It must be noted that any other appropriate party can as well act as a certificate service provider. It is also possible, however not depicted in the figures, that the security gateway is managed by the service provider and that the certificate service provider functions are provided by the service provider itself. Furthermore, it is possible that the service provider acts also as a certificate service provider, and therefore, a distinct trusted third party is not needed. Although it is described in Figures 1 - 9 that the terminal devices DTE, DTE2 are mobile phones, they can be any other appropriate terminal devices. Moreover, although it has been described that the mobile phone and/or security gateway use(s) PKCS#1 or PKCS#7 messages in validation messaging, PKCS#1 and PKCS#7 messages are used only as examples and any other appropriate messages can be used.

The present invention describes a solution wherein a logical channel (e.g. a call connection) is set up between a caller terminal and a service provider. The problem is how to reliably verify the identity of the caller. Therefore, in accordance with the present invention the caller is authenticated via a another preferably secured logical channel between the service provider and the caller terminal prior to providing any services to the caller via the established call connection. The transmission channel itself is known to a man skilled in the art and refers e.g. to a connectionless packet data connection via a mobile communication network or a packet connection using the secure and standardized GSM feature described e.g. in

29

the ETSI TS 101 181 V8.8.0 (2001-12) publication. However, the transmission channel may also refer to a circuit switched connection.

Furthermore, the present invention provides a
5   secure solution for identification, authentication, validation and authorization of a user via two logical channels.

It is obvious to a person skilled in the art that with the advancement of technology, the basic
10   idea of the invention may be implemented in various ways. The invention and its embodiments are thus not limited to the examples described above, instead they may vary within the scope of the claims.

30

L 3

CLAIMS

1. A method for authenticating a user of a first terminal in a communication system,

·c h a r a c t e r i z e d   in that the method
5   comprises the steps of:

setting up a first logical channel via a communication network between a first terminal and a service provider; and

identifying the identity of the user of the first
10   terminal after the first logical channel set up via a second logical channel other than the established first logical channel between the service provider and the first terminal prior to providing any services to the user of the first terminal.

15   2. The method according to claim 1, c h a r -
a c t e r i z e d   in that the method further comprises the steps of:

sending a user identification request from the service provider to the first terminal via the second
20   logical channel while the first logical channel exists between the first terminal and the service provider;

receiving the user identification request with the first terminal while the first logical channel exists;

digitally signing the request;
25   sending the signed request with the first terminal via the second logical channel;

authenticating the user of the first terminal and verifying the digital signature; and

providing the user with services provided by the
30   service provider via the first logical channel.

3. The method according to claim 1, c h a r -
a c t e r i z e d   in that the method further comprises the steps of:

sending a user identification request for the user
35   of the first terminal from the service provider to a second terminal via the second logical channel while

31

the first logical channel exists between the first
terminal and the service provider;

receiving the user identification request with the
second terminal while the first logical channel ex-
5   ists;

digitally signing the request;

sending the signed request with the second termi-
nal via the second logical channel;

authenticating the user of the second terminal and
10   verifying the digital signature; and

providing the user of the first terminal with
services provided by the service provider via the
first logical channel.

4. The method according to claim 1, c h a r -
15   a c t e r i z e d   in that the method further comprises
the steps of:

sending a user identification request for the user
of the first terminal from the service provider to a
second terminal via the second logical channel, the
20   user identification request comprising also a chal-
lenge;

receiving the user identification request compris-
ing the challenge with the second terminal;

digitally signing the request comprising the chal-
25   lenge;

sending the signed request with the second termi-
nal via the second logical channel;

providing the user of the first terminal with the
challenge with the second terminal;

30   providing the service provider with the challenge
acquired from the user of the second terminal;

comparing the challenge in the signed message from
the second terminal and the challenge provided by the
user of the first terminal; and if the challenges are
35   equal,

authenticating the user of the second terminal and
verifying the digital signature; and

32

providing the user of the first terminal with services provided by the service provider via the first logical channel.

5. The method according to claim 1, 2, 3 or
5 4, c h a r a c t e r i z e d in that the first and/or second logical channel refers to a packet switched connection.

6. The method according to claim 1, 2, 3 or
4, c h a r a c t e r i z e d in that the first and/or
10 second logical channel refers to a circuit switched connection.

7. The method according to claim 1, 2, 3 or
4, c h a r a c t e r i z e d in that the method further comprises the step of:
15 arranging a security gateway forming an interface towards the first and/or second terminal.

8. The method according to claim 7, c h a r -
a c t e r i z e d in that the method further comprises the steps of:
20 identifying the service provider with the security gateway;

sending a user identification request from the service provider to the security gateway;

sending the user identification request from the
25 security gateway to the first terminal via the second logical channel;

receiving the identification request with the first terminal;

digitally signing the request;
30 sending the signed request to the security gateway via the second logical channel;

retrieving a certificate related to the user of the first terminal;

authenticating the identity of the user of the
35 first terminal and verifying the digital signature; and

33

providing the user of the first terminal a service provided by the service provider via the existing first logical channel.

9. The method according to claim 7, c h a r -
5 a c t e r i z e d in that the method further comprises the steps of:

identifying the service provider with the security gateway;

sending a user identification request of the user
10 of the first terminal from the service provider to the security gateway;

sending the user identification request from the security gateway to a second terminal via the second logical channel;

15 receiving the user identification request with the second terminal;

digitally signing the request;

sending the signed request to the security gateway via the second logical channel;

20 retrieving a certificate related to the user of the second terminal;

authenticating the identity of the user of the second terminal and verifying the digital signature; and

25 providing the user of the first terminal a service provided by the service provider via the existing first logical channel.

10. The method according to claim 2, 3, 4, 8 or 9, c h a r a c t e r i z e d in that the method fur-
30 ther comprises the step of:

encrypting the user identification request sent to the first and/or second terminal using symmetric or asymmetric encryption; and

encrypting the signed request sent from the first
35 and/or second terminal using symmetric or asymmetric encryption.

34

11. The method according to claim 8 or 9, c h a r a c t e r i z e d in that the method further comprises the step of:

encrypting the signed user identification request
5 sent to the security gateway using symmetric or asymmetric encryption.

12. The method according to claim 8 or 9, c h a r a c t e r i z e d in that the method further comprises the steps of:
10 retrieving with the security gateway a certificate related to the user of the first and/or second terminal;

creating and sending a validating message to the service provider; and
15 validating the user of the first and/or second terminal with the service provider based on the validating message and validating information.

13. The method according to claim 8 or 9, c h a r a c t e r i z e d in that the method further
20 comprises the steps of:

retrieving with the security gateway validation information comprising at least a certificate related to the user of the first and/or second terminal;

authenticating the identity of the user of the
25 first and/or second terminal with the security gateway based on the validation information; and

sending a positive validation message to the service provider if the result of the validation was positive.

30 14. The method according to claim 1, c h a r a c t e r i z e d in that if the first logical channel fails during the validation procedure, the method further comprises the steps of:

creating a challenge;
35 encrypting the challenge with the public encryption key of the user of the first terminal;

35

sending the encrypted challenge to the first terminal;

decrypting the encrypted challenge in the first terminal;

5   setting up a new logical channel to the service provider;

providing the service provider with the decrypted challenge; and if the challenge is acceptable,

providing the user of the first terminal via the
10   logical channel with a service provided by the service provider.

15. The method according to claim 14, c h a r a c t e r i z e d in that the method further comprises the step of:

15   sending the encrypted challenge to the first terminal via a security gateway.

16. A system for authenticating a user of a first terminal in a communication system, the system comprising:

20   a communication network (NET),

a first terminal (DTE) associated with the communication network (NET),

a service provider (SP) associated with the communication network (NET),

25   a certificate service provider (CA),

c h a r a c t e r i z e d in that the system further comprises:

sending means (SM) for sending a user identification request to the first terminal (DTE) or a second
30   terminal (DTE2); and

identifying means (ID) for identifying the identity of the user of the first terminal (DTE) after a first logical channel has been set up via a second logical channel other than the established first logi-
35   cal channel between the service provider and the first terminal (DTE) prior to providing any services to the user of the first terminal (DTE) based on the informa-

36

tion provided by the certificate service provider
(CA).

    17. The system according to claim 16,
c h a r a c t e r i z e d   in that the system further
5 comprises:

    a security gateway (GW) in connection with the
service provider (SP) and certificate service provider
(CA).

    18. The system according to claim 17,
10 c h a r a c t e r i z e d   in that the security gateway
(GW) is managed by the service provider (SP).

    19. The system according to claim 17,
c h a r a c t e r i z e d   in that the security gateway
(GW) is managed by a third party.

15   20. The system according to claim 16,
c h a r a c t e r i z e d   in that said sending means
(SM) are arranged in the service provider (SP).

    21. The system according to claim 16 or 17,
c h a r a c t e r i z e d   in that said sending means
20 (SM) are arranged in the service provider (SP) and se-
curity gateway (GW).

    22. The system according to claim 16 or 17,
c h a r a c t e r i z e d   in that said identifying means
(TD) are arranged in the service provider (SP) and/or
25 security gateway (GW).

    23. The system according to claim 16,
c h a r a c t e r i z e d   in that the service provider
(SP) comprises:

    first encrypting means (EN1) for encrypting infor-
30 mation; and

    first decrypting means (DE1) for decrypting infor-
mation.

    24. The system according to claim 17,
c h a r a c t e r i z e d   in that the security gateway
35 (GW) comprises:

    second encrypting means (EN2) for encrypting in-
formation; and

37

second decrypting means (DE2) for decrypting information.

25. The system according to claim 16, c h a r a c t e r i z e d in that the first terminal (DTE) and/or second terminal (DTE2) comprises:

third encrypting means (EN3) for encrypting information; and

third decrypting means (DE3) for decrypting information.

26. The system according to claim 20 or 21, c h a r a c t e r i z e d in that said sending means (SM) are arranged to send a challenge to the first terminal (DTE) in the event that the logical channel set up between the first terminal (DTE) and service provider (SP) fails.

27. The system according to claim 20 or 21, c h a r a c t e r i z e d in that said sending means (SM) are arranged to send a challenge to the second terminal (DTE2).

28. The system according to any of the claims 16 - 27, c h a r a c t e r i z e d in that the communication network is a GSM network.

29. The system according to any of the claims 16 - 27, c h a r a c t e r i z e d in that the communication network is a GSM network with the GPRS feature.

30. The system according to any of the claims 16 - 27, c h a r a c t e r i z e d in that the communication network is an UMTS, a CDMA, a WCDMA, an EDGE, a Bluetooth, or a WLAN network.

L4   /

(57) ABSTRACT

The present invention describes
a method and system for verifying the
identity of a user of a first terminal
in a communication system comprising at

5   least a communication network (NET), a
first terminal (DTE) associated with the
communication network (NET) and a serv-
ice provider (SP) associated with the
communication network (NET). In the

10   method, a first logical channel is set
up via the communication network between
the first terminal (DTE) and the service
provider (SP). The user of the first
terminal is identified after the first

15   logical channel set up via a second
logical channel other than the estab-
lished first logical channel between the
service provider and the first terminal
prior to providing any services to the

20   caller.

(FIG. 1)

L 5

1

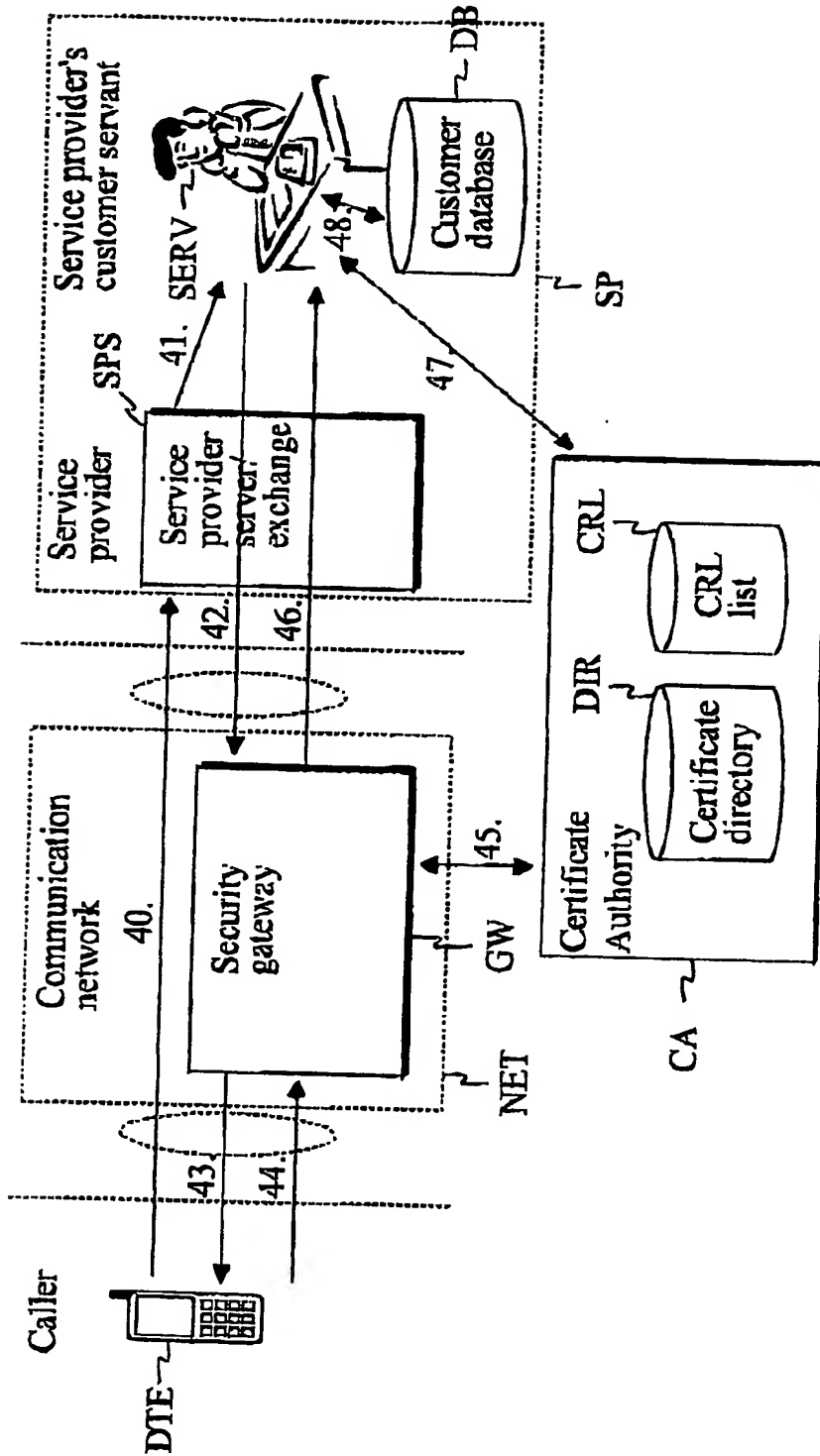
Fig. 1

L5

2

Fig.2

L5

3

Fig. 3

L5

4

Fig. 4

L 5

5

Fig. 5
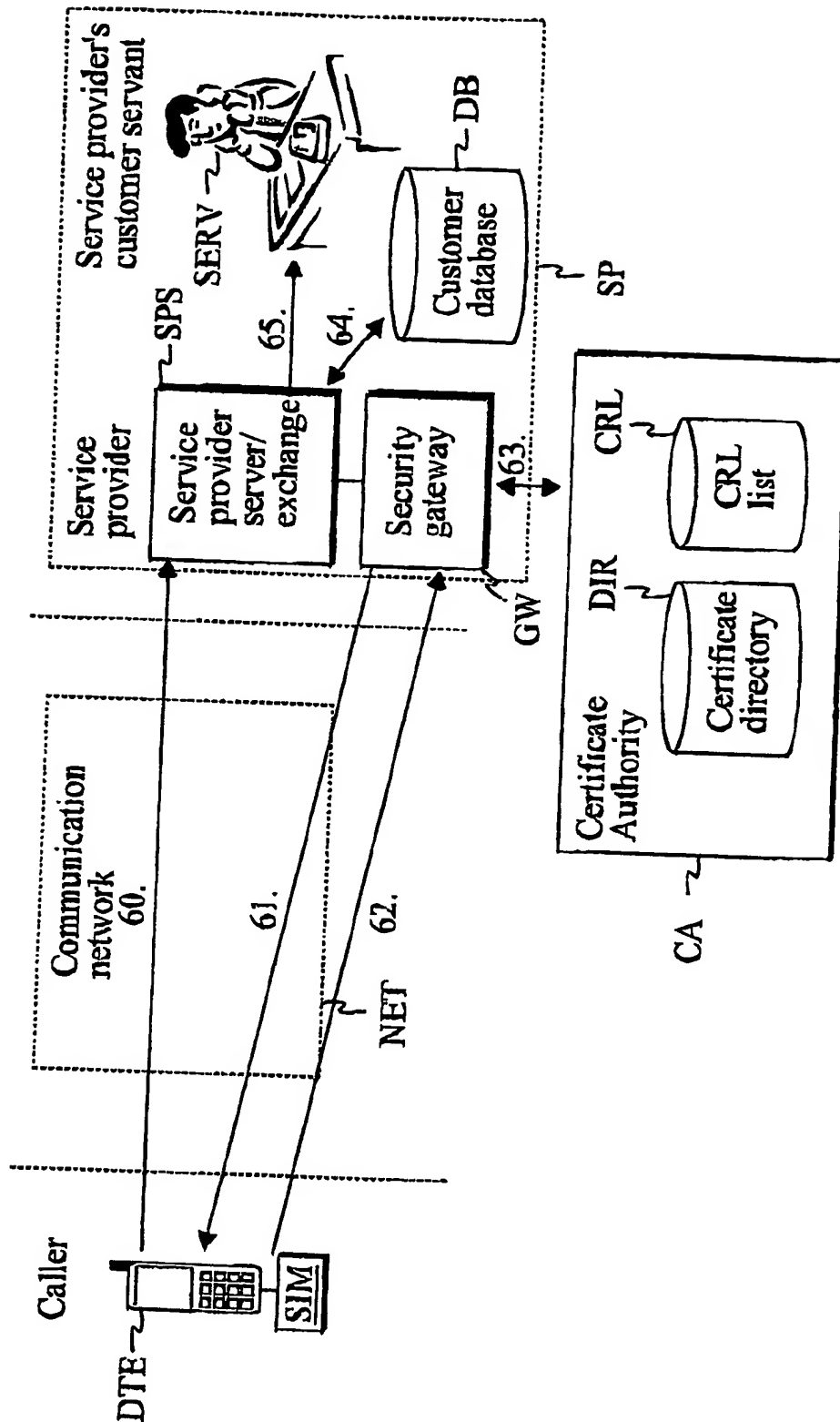
Fig. 6

LS   7

Fig. 7

Fig. 8

L 5

9

Fig. 9